UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/041,964	01/09/2002	Makoto Oka	SON-2320	4260

7590 11/27/2007

RADER, FISHMAN & GRAUER, P.L.L.C.
Suite 501
1233 20th Street, NW
Washington, DC 20036

EXAMINER	
POWERS, WILLIAM S	

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
11/27/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/041,964
Filing Date: January 09, 2002
Appellant(s): OKA ET AL.

Ronald P. Kananen
Registration No. 24,104

Christopher M. Tobin
Registration No. 40,290

For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed September 4, 2007 appealing from the Office action mailed April 12, 2007.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,035,402	Vaeth et al.	3-2000
6,202,157	Brownlie et al.	3-2001
6,675,296	Boeyen et al.	1-2004

Boneh et al. "On the Importance of Checking Cryptographic Protocols for Faults" Advances in Cryptology- EUROCRYPT '97, LNCS 1233, pp. 37-51, 1997. Springer-Verlag Berlin Heidelberg.

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-3, 5, 6, 9, 10, 12-17, 19, 20, 22-25, 27, 28, 31, 32 and 34-36 are rejected under 35 U.S.C. 102(b) as being anticipated by US Patent 6,035,402 to Vaeth, et al. (hereinafter Vaeth).

As to claims 1, 14, 23 and 36 Vaeth teaches:

a. A certificate authority for issuing a public key certificate used by an entity (column 8, lines 35-48).

b. A registration authority which, on receiving a public key certificate issuance request from any one of entities under jurisdiction thereof, transmits the received request to said certificate authority (column 8, lines 35-48).

c. Wherein said certificate authority, having a plurality of signature modules (crypto cards) each executing a different encryption algorithm (column 7, lines 41-47), selects at least one of said plurality of signature modules in accordance with said public key certificate issuance request from said registration authority based upon an identification of an assigned encryption algorithm, said identification of the assigned algorithm being made with reference to a table that associates the registration authority with an the assigned encryption algorithm, and causes the selected signature module to attach a digital signature to message data constituting a public key certificate (Different functions (e.g. cardholders, merchants) have different crypto cards associated with them as well as different registration authorities, the RA verifies the certificate request of the users through a registration database. Once a request is approved, it is forwarded by the RA to the CA and the RA is thus associated with the user, crypto card and private keys used by the CA to sign and encrypt the requested certificate.) (column 7, lines 41-47 and column 8, line 35-column 9, line 12).

As to claims 2 and 24, Vaeth teaches:

a. Said certificate authority has a certificate authority server for outputting a signature processing request to said plurality of signature modules (column 9, lines 24-31).

b. Wherein said certificate authority server receives said public key certificate issuance request from said registration authority, selects at least one of said plurality of signature modules in response to said public key certificate issuance request, and outputs said signature processing request to the selected signature module (column 9, lines 24-45).

c. Wherein each selected signature module attaches a digital signature to the message data constituting said public key certificate in response to said signature processing request received from said certificate authority server (column 7, lines 41-47).

As to claims 3 and 25, Vaeth teaches:

a. Said certificate authority has a registration authority management database which stores registration authority management data for associating registration authorities issuing public key certificate issuance requests with an encryption algorithm specific to each of said registration authorities (different functions (e.g. cardholders, merchants) have different crypto cards associated with them as well as different registration authorities and these associations are determined through screening functions performed by the CA) (column 7, lines 41-47 and column 8, line 49-column 9, line 12).

b. Wherein, given a public key certificate issuance request from any registration authority, said certificate authority selects the signature module associated with the relevant encryption algorithm based on said registration authority management data (different functions (e.g. cardholders, merchants) have different crypto cards associated with them as well as different registration authorities and these associations are determined through screening functions performed by the CA) (column 7, lines 41-47 and column 8, line 49-column 9, line 12).

As to claims 5 and 27, Vaeth teaches said registration authority management data include signature module identification information applicable to signatures (different functions (e.g. cardholders, merchants) have different crypto cards associated with them as well as different registration authorities, these associations are determined through screening functions performed by the CA and thereby the proper signature is applied to the certificate as dictated by the associated RA) (column 7, lines 41-47 and column 8, line 49-column 9, line 12).

As to claims 6 and 28, Vaeth teaches:

a. Said registration authority transmits encryption algorithm designation information along with said public key certificate issuance request to said certificate authority (the algorithm designation information is the RA itself and the associations are determined through screening functions performed by the CA and thereby the proper signature is applied to the certificate as dictated by the associated RA) (column 7, lines 41-47 and column 8, line 49-column 9, line 12).

b. Wherein said certificate authority, based on said encryption algorithm designation information received along with said public key certificate issuance request, selects a signature module applicable to the designated encryption algorithm (Different functions (e.g. cardholders, merchants) have different crypto cards associated with them as well as different registration authorities, the RA verifies the certificate request of the users through a registration database. Once a request is approved, it is forwarded by the RA to the CA and the RA is thus associated with the user, crypto card and private keys used by the CA to sign and encrypt the requested certificate.) (column 7, lines 41-47 and column 8, line 35-column 9, line 12).

As to claims 9, 19 and 31, Vaeth teaches said certificate authority uses at least two of said plurality of signature modules to attach at least two different digital signatures to one public key certificate (joint approval scheme) (column 8, lines 49-59).

As to claims 10, 20 and 32, Vaeth teaches said certificate authority selects at least two of said plurality of signature modules in order to have signature processing executed in steps by each of the selected signature modules used in concert for digital signature generation (joint approval scheme) (column 8, lines 49-59).

As to claims 12 and 34, Vaeth teaches at least part of said plurality of signature module have a common signature key stored therein (storage of the CA's private keys) (column 6, lines 32-39).

As to claims 13, 22 and 35, as best understood by the Examiner, Vaeth teaches each of said selected signature modules is configured to execute multiple encryption algorithms (column 8, lines 49-59).

As to claim 15, Vaeth teaches:

a. Causing a certificate authority server to receive a public key certificate issuance request from said registration authority (column 9, lines 24-31).

b. Causing said certificate authority server to select at least one of said plurality of signature modules in response to said public key certificate issuance request (column 9, lines 24-45).

c. Causing said certificate authority server to output a signature processing request to the selected signature module (column 7, lines 41-47).

As to claim 16, Vaeth teaches said step involving said certificate authority server selecting the signature module comprises selecting the signature module based on a registration authority management database which stores registration authority management data for associating registration authorities issuing public key certificate issuance requests with an encryption algorithm specific to each of said registration authorities (Different functions (e.g. cardholders, merchants) have different crypto cards associated with them as well as different registration authorities, the RA verifies the certificate request of the users through a registration database. Once a request is approved, it is forwarded by the RA to the CA and the RA is thus associated with the user, crypto card and private keys used by the CA to sign and encrypt the requested certificate.) (column 7, lines 41-47 and column 8, line 35-column 9, line 12).

As to claim 17, Vaeth teaches said step involving said certificate authority server selecting the signature module comprises selecting the signature module based on encryption algorithm designation information received along with said public key certificate issuance request (different functions (e.g. cardholders, merchants) have different crypto cards associated with them as well as different registration authorities and these associations are determined through screening functions performed by the CA) (column 7, lines 41-47 and column 8, line 49-column 9, line 12).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

5. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

6. Claim 4 and claim 7 and claim 26 and claim 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,035,402 to Vaeth, et al. (hereinafter Vaeth) as applied to claim 1 and claim 6 and claim 25 and claim 28 above respectively in view of US Patent No. 6,202,157 to Brownlie et al. (hereinafter Brownlie).

As to claims 4 and 26, Vaeth does not expressly mention storing the key length and parameter data of the signatures in a database. However, in an analogous art, Brownlie teaches management data that includes key length and parameter information applicable to signatures (Brownlie, column 3, lines 25-49).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the certificate system of Vaeth with the storing of parameter information of the signature algorithms of Brownlie in order to "allow enforcement of the policies to occur at the network nodes to help reduce overhead requirements of a central authority," as suggested by Brownlie (Brownlie, column 2, lines 31-33).

As to claims 7 and 29, Vaeth as modified teaches said encryption algorithm designation information includes key length and parameter information applicable to signatures (Brownlie, column 3, lines 25-49).

7. Claim 8 and claim 18 and claim 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,035,402 to Vaeth, et al. (hereinafter Vaeth) as applied to

claim 1 and claim 14 and claim 23 respectively above, and further in view of "On the Importance of Checking Cryptographic Protocols for Faults," by Boneh et al. (hereinafter Boneh).

As to claims 8, 18 and 30, Vaeth teaches:

a. Said certificate authority has a verification key database which stores signature keys of the crypto cards and certificates (crypto cards (column 6, lines 32-38) and RAID array to store CRDs and certificates (column 10, lines 34-36)).

Vaeth does not expressly mention the verifying of the certificate authority signatures by the certificate authority. However, in an analogous art, Boneh teaches said certificate authority verifies signatures generated by each of said plurality of signature modules (Boneh, page 38, lines 28-34).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the certificate system of Vaeth with the signature verification of Boneh in order to maintain the security of the certificate authority and prevent the generation of fake certificates as suggested by Boneh (Boneh, page 37, lines 11-17).

8. Claim 11 and claim 21 and claim 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,035,402 to Vaeth, et al. (hereinafter Vaeth) as applied to claim 1 and claim 14 and claim 23 respectively above, and further in view of US Patent No. 6,675,296 to Boeyen et al. (hereinafter Boeyen).

As to claims 11, 21 and 33, Vaeth teaches that registration authorities are associated with respective crypto cards (signature modules) and the appropriate signature is attached to the certificate (column 8, lines 35-59), but does not expressly mention the use of identifiers. However, in an analogous art, Boeyen teaches certificate generator that has a digital format selector (identifier) that is used in selecting the proper signature from the certificate template data (Boeyen, column 6, line 62-column 7, line 18).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the certificate system of Vaeth with the signature selector of Boeyen in order to ensure that the proper signature type is attached to a certificate.

(10) Response to Argument

Applicant's arguments, see Appeal Brief, pages 8-15, filed 9/4/2007, with respect to claims 1-36 have been fully considered and are not persuasive.

Claims 1-4 and 8-13

In response to Applicant's remark that, "[t]here is no mention or suggestion that the applicable crypto-card is based on the RA associated with a given requesting entity" (Remarks, page 10, lines 14-15), the Examiner respectfully disagrees. The Board's attention is directed to column 7, lines 23-28 of the Vaeth patent that expressly states that a Registration Authority (RA) may be associated with a credit card issuer while another RA may be associated with a corporate account authorization office. The RA is not generic entity as alleged by the Applicant. Vaeth further points out, "In yet another alternative embodiment, the CA 190 may notify appropriate RAs of its receipt of a CRD [certificate request and data]" (column 8, lines 32-34). It is important to note that the "appropriate RAs" are notified so that the user submitted data for a certificate request can be verified. The RAs are involved in the certificate creation and granting activities of Vaeth. Vaeth repeatedly associates specific RAs with specific responsibilities (card issuer, corporate charge accounts). The RAs act as "virtual CAs" (Vaeth, column 7, lines 64-65), and although a single RA can be used for approval of three different types of certificates (Vaeth, column 9, lines 5-9), the RA acts as a different "virtual CA" to the CA for each of the different kinds of approval. The RA, in affect, assumes the role of the requestor in the approval scheme and causes the CA to apply the appropriate digital signature executed by the various cryptographic cards (crypto cards) in the CA of Vaeth. For at least the reasons above the rejection to claims 1-4 and 8-13 is maintained.

In response to Applicant's remark that, "Vaeth does not teach or suggest 'a table that associates the registration authority with the assigned encryption algorithm'" (Remarks, page 10, lines 23-24), the Examiner respectfully disagrees. The Examiner sees the table of the instant application as a representation of an association between a registration authority and a signature algorithm. As such, Vaeth does teach an association between a registration authority and a signature algorithm in the form of a crypto card. The CA of Vaeth "can support a different brand of credit card with a different RA acting as a different 'virtual CA' using a different crypto card," (Vaeth, column 9, lines 9-12). In this case a different RA is associated with a different crypto card. The RAs have specific responsibilities such as at least corporate charge accounts, credit card issuers and merchant accounts. For at least the reasons above, the rejection to claims 1-4 and 8-13 is maintained.

Claim 5

In response to Applicant's remark that, "Vaeth fails to disclose, teach or suggest wherein said registration authority management data include signature module identification information applicable to signatures" (Remarks, page 12, lines 1-3), the Examiner respectfully disagrees. The Applicant states, "Vaeth clearly teaches that multiple entities **can** use the same RA to request different types of certificates from the

Certificate Authority" (Remarks, page 11, lines 22-23) (emphasis added). There is nothing in the claim language that requires the RA to be associated with only one signature module or that the RA cannot request different types of certificates. The Vaeth patent allows for the possibility that the same RA **can** request different certificates Vaeth states, "[e]ach of the approvals for these three different types of certificates might be performed by the same RA 180, for example the credit card issuer, acting as a different 'virtual CA' (using a different crypto card) for each type of certificate" (Vaeth, column 9, lines 5-9). Even if the Vaeth patent restricted all entities to go through one RA to request certificates from a CA, the RA differentiates itself to the CA by "acting as a different 'virtual CA'". The RA of Vaeth **can** request different certificates, but the CA sees the RA acting in a different role according to the requesting entity and applies the appropriate signature module to the requested certificate. For at least the reasons above, the rejection of claim 5 is maintained.

Claims 6 and 7

In response to Applicant's remark that, "Vaeth does not disclose employing information from an RA to decide which crypto-card to use to produce a given certificate" (Remarks, page 12, lines 9-10), the Examiner respectfully disagrees. The RAs of Vaeth act as "virtual CAs" (Vaeth, column 7, lines 64-65) and as such convey information supplied by the requesting entity to CA for the appropriate certificate with the appropriate signature. In Vaeth, there are different functions for cardholders, merchants and payment gateways and they require different crypto cards to generate the needed certificates (Vaeth, column 7, lines 33-47). The CA responds to requests through RAs associated with the above mentioned functions. The RAs determine the necessary information needed for the requested certificate when they are acting as the "virtual CA" (Vaeth, column 7, line 66-column 8, line 6). It is through the RA that the CA obtains the data needed to generate the certificate, including the correct signature created by the appropriate crypto card. For at least the reasons above, the rejection of claims 6 and 7 is maintained.

Claims 14-15 and 17-22

In response to Applicant's remark that, "Vaeth fails to disclose, teach or suggest ... a table that associates the registration authority with the assigned encryption algorithm" (Remarks, page 12, lines 19-25), the Examiner respectfully disagrees. The Examiner sees the table of the instant application as a representation of an association between a registration authority and a signature algorithm. As such, Vaeth does teach an association between a registration authority and a signature algorithm in the form of a crypto card. The CA of Vaeth "can support a different brand of credit card with a different RA acting as a different 'virtual CA' using a different crypto card," (Vaeth, column 9, lines 9-12). In this case a different RA is associated with a different crypto card. The RAs have specific responsibilities such as at least corporate charge accounts, credit card issuers and merchant accounts. For at least the reasons above, the rejection to claims 14-15 and 17-22 is maintained.

Claim 16

In response to Applicant's remark that, "[i]n Vaeth, the Certification Authority (CA) produces the type of certificates based on the requesting entities, not based on signature module information from the RA" (Remarks, page 13, lines 1-3), the Examiner respectfully disagrees. The Vaeth patent allows for the possibility that the same RA **can** request different certificates Vaeth states, "[e]ach of the approvals for these three different types of certificates might be performed by the same RA 180, for example the credit card issuer, acting as a different 'virtual CA' (using a different crypto card) for each type of certificate" (Vaeth, column 9, lines 5-9). Even if the Vaeth patent restricted all entities to go through one RA to request certificates from a CA, which it does not, the RA differentiates itself to the CA by "acting as a different 'virtual CA'". The RA of Vaeth can request different certificates, but the CA sees the RA acting in a different role according to the requesting entity and applies the appropriate signature module to the requested certificate and it is through the information and verification provided by the RA that the entity receives the certificate. For at least the reasons above, the rejection of claim 16 is maintained.

Claims 23-26 and 30-35

In response to Applicant's remark that, "Vaeth fails to teach or suggest that the type of certificate produced by the Certification Authority (CA) is based on a Registration Authority (RA)" (Remarks, page 13, lines 10-12), the Examiner respectfully disagrees. The Board's attention is directed to column 7, lines 23-28 of the Vaeth patent that expressly states that a Registration Authority (RA) may be associated with a credit card issuer while another RA may be associated with a corporate account authorization office. The RA is not generic entity as alleged by the Applicant. Vaeth further points out, "In yet another alternative embodiment, the CA 190 may notify appropriate RAs of its receipt of a CRD [certificate request and data]" (column 8, lines 32-34). It is important to note that the "appropriate RAs" are notified so that the user submitted data for a certificate request can be verified. The RAs are involved in the certificate creation and granting activities of Vaeth. Vaeth repeatedly associates specific RAs with specific responsibilities (card issuer, corporate charge accounts). The RAs act as "virtual CAs" (Vaeth, column 7, lines 64-65), and although a single RA can be used for approval of three different types of certificates (Vaeth, column 9, lines 5-9), the RA acts as a different "virtual CA" to the CA for each of the different kinds of approval. The RA, in affect, assumes the role of the requestor in the approval scheme and causes the CA to apply the appropriate digital signature executed by the various cryptographic cards (crypto cards) in the CA of Vaeth. For at least the reasons above the rejection to claims 23-26 and 30-35 is maintained.

In response to Applicant's remark that, "Vaeth does not teach or suggest ... a table that associates the registration authority with the assigned encryption algorithm" (Remarks, page 13, lines 13-22), the Examiner respectfully disagrees. The Examiner sees the table of the instant application as a representation of an association between a registration authority and a signature algorithm. As such, Vaeth does teach an association between a registration authority and a signature algorithm in the form of a crypto card. The CA of Vaeth "can support a different brand of credit card with a different RA acting as a different 'virtual CA' using a different crypto card," (Vaeth, column 9, lines 9-12). In this case a different RA is associated with a different crypto card. The RAs have specific responsibilities such as at least corporate charge accounts, credit card issuers and merchant accounts. For at least the reasons above, the rejection to claims 23-26 and 30-35 is maintained.

Claim 27

In response to Applicant's remark, "[i]n Vaeth, the Certification Authority (CA) produces the type of certificates based on the requesting entities, not based on signature module information from the RA" (Remarks, page 13, lines 23-25), the Examiner respectfully disagrees. Vaeth states, "[e]ach of the approvals for these three different types of certificates might be performed by the same RA 180, for example the credit card issuer, acting as a different 'virtual CA' (using a different crypto card) for each type of certificate" (Vaeth, column 9, lines 5-9). Even if the Vaeth patent restricted all entities to go through one RA to request certificates from a CA, the RA differentiates itself to the CA by "acting as a different 'virtual CA'". The RA of Vaeth **can** request different certificates, but the CA sees the RA acting in a different role according to the requesting entity and applies the appropriate signature module to the requested certificate. For at least the reasons above, the rejection of claim 27 is maintained.

Claims 28 and 29

In response to Applicant's remark that, "Vaeth does not disclose using information from the RA to determine which encryption algorithm to use to produce [a] given type of certificate" (Remarks, page 14, lines 1-2), the Examiner respectfully disagrees. The Board's attention is directed to column 7, lines 23-28 of the Vaeth patent that expressly states that a Registration Authority (RA) may be associated with a credit card issuer while another RA may be associated with a corporate account authorization office. The RA is not generic entity as alleged by the Applicant. Vaeth further points out, "In yet another alternative embodiment, the CA 190 may notify appropriate RAs of its receipt of a CRD [certificate request and data]" (column 8, lines 32-34). It is important to note that the "appropriate RAs" are notified so that the user submitted data for a certificate request can be verified. The RAs are involved in the certificate creation and granting activities of Vaeth. Vaeth repeatedly associates specific RAs with specific responsibilities (card issuer, corporate charge accounts). The RAs act as "virtual CAs"

(Vaeth, column 7, lines 64-65), and although a single RA can be used for approval of three different types of certificates (Vaeth, column 9, lines 5-9), the RA acts as a different "virtual CA" to the CA for each of the different kinds of approval. The RA, in affect, assumes the role of the requestor in the approval scheme and causes the CA to apply the appropriate digital signature executed by the various cryptographic cards (crypto cards) in the CA of Vaeth. For at least the reasons above the rejection to claims 28 and 29 is maintained.

Claim 36

In response to Applicant's remark that, "Vaeth fails to teach or suggest that the type of certificate produced by the Certification Authority (CA) is based on the requesting Registration Authority (RA)" (Remarks, page 14, lines 7-9), the Examiner respectfully disagrees. Vaeth states, "[e]ach of the approvals for these three different types of certificates might be performed by the same RA 180, for example the credit card issuer, acting as a different 'virtual CA' (using a different crypto card) for each type of certificate" (Vaeth, column 9, lines 5-9). Even if the Vaeth patent restricted all entities to go through one RA to request certificates from a CA, the RA differentiates itself to the CA by "acting as a different 'virtual CA'". The RA of Vaeth **can** request different certificates, but the CA sees the RA acting in a different role according to the requesting entity and applies the appropriate signature module to the requested certificate. For at least the reasons above, the rejection of claim 36 is maintained.

Claims 4, 7, 26 and 29

In response to Applicant's remark that, "Brownlie fails to teach or suggest a certification scheme that associates the registration authority with an assigned encryption algorithm" (Remarks, page 14, lines 21-22), the Examiner points out that the Brownlie patent is not relied upon for that limitation. Therefore, the arguments are considered moot. Arguments to the cited limitations are addressed above. For at least the reasons above, the rejection of claims 4, 7, 26 and 29 is maintained.

Claims 8, 18 and 30

In response to Applicant's remark that, "Boneh fails to disclose, teach or suggest that said identification of the assigned algorithm [is] made with reference to a table that associates the registration authority with the assigned encryption algorithm" (Remarks, page 15, lines 8-10), the Examiner points out that the Boneh publication is not relied upon for that limitation. Therefore, the arguments are considered moot. Arguments to the cited limitations are addressed above. For at least the reasons above, the rejection of claims 8, 18 and 30 is maintained.

Claims 11, 21 and 33

In response to Applicant's remark that, "Boeyen fails to disclose, teach or suggest that said identification of the assigned algorithm [is] made with reference to a table that associates the registration authority with the assigned encryption algorithm" (Remarks, page 15, 20-22), the Examiner points out that the Boeyen patent is not relied upon for that limitation. Therefore, the arguments are considered moot. Arguments to the cited limitations are addressed above. For at least the reasons above, the rejection of claims 11, 21 and 33 is maintained.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER

William S. Powers

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Conferees:

Kambiz Zand

Kim Vu

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER